CLAIMS

WHAT IS CLAIMED:

1. A communications system, comprising:

a physical layer hardware unit adapted to communicate data over a communications channel in accordance with assigned transmission parameters, the physical layer hardware unit being adapted to receive an incoming signal over the communications channel and sample the incoming signal to generate a digital received signal; and

a processing unit adapted to execute a software driver including program instructions adapted to extract control codes from the digital received signal, generate an authentication code, and transfer the control codes and the authentication code to the physical layer hardware unit, wherein the physical layer hardware unit is adapted to signal a security violation in response to the control codes being inconsistent with the authentication code.

2. The system of claim 1, wherein the authentication code comprises a hidden authentication code.

3. The system of claim 1, wherein the software driver includes program instructions adapted to transfer the authentication code out-of-band with respect to the control codes.

4. The system of claim 3, wherein the processor complex includes a data bus, and the software driver includes program instructions adapted to transfer the authentication code on an unused portion of the data bus.

5. The system of claim 3, wherein the processing unit includes a data bus adapted to transfer data in frames having a fixed number of slots, and the software driver includes program instructions adapted to transfer the authentication code using a frame having more slots than the fixed number of slots.

6. The system of claim 1, wherein the software driver includes program instructions adapted to extract encrypted data from the digital received signal and decrypt the encrypted data to generate decrypted data including the control codes.

7. The system of claim 6, wherein the software driver includes program instructions adapted to generate the authentication code based on the decrypted data.

8. The system of claim 1, wherein the assigned transmission parameters include at least one of a power level assignment, a frequency assignment, and a time slot assignment.

9. The system of claim 1, wherein the processing unit comprises a computer.

10. The system of claim 9, wherein the computer includes:

a processor complex adapted to execute the program instructions in the software driver;

a bus coupled to the processor complex; and

an expansion card coupled to the bus, the expansion card including the physical layer hardware.

11. The system of claim 1, wherein the physical layer hardware unit is adapted to prohibit at least some communication over the communications channel in response to identifying the security violation.

12. A method for identifying security violations in a transceiver, comprising:

receiving digital data over a communications channel;

extracting control codes from the digital received signal;

generating an authentication code;

transferring the control codes and the authentication code to a physical layer hardware unit of the transceiver;

configuring assigned transmission parameters of the physical layer hardware unit based on the control codes; and

signaling a security violation in response to the control codes being inconsistent with the authentication code.

13. The method of claim 12, wherein generating the authentication code further comprises generating a hidden authentication code.

14. The method of claim 12, wherein transferring the control codes and the authentication code comprises transferring the authentication code out-of-band with respect to the control codes.

15. The method of claim 14, wherein transferring the control codes and the authentication code comprises transferring the authentication code on an unused portion of a data bus communicating with the transceiver.

16. The method of claim 14, wherein the transceiver is coupled to data bus adapted to transfer data in frames having a fixed number of slots, and transferring the control codes and the authentication code comprises transferring the authentication code using a frame having more slots than the fixed number of slots.

17. The method of claim 12, further comprising:

extracting encrypted data from the digital received signal; and

decrypting the encrypted data to generate decrypted data including the control codes.

18. The method of claim 17, wherein generating the authentication code comprises generating the authentication code based on the decrypted data.

19. The method of claim 12, wherein configuring assigned transmission parameters of the physical layer hardware unit based on the control codes comprises configuring at least one of a power level parameter, a frequency parameter, and a time slot parameter.

20. The method of claim 12, further comprising prohibiting communication over the communications channel in response to identifying the security violation.

21. A modem, comprising:

means for receiving digital data over a communications channel;

means for extracting control codes from the digital received signal;

means for generating an authentication code;

means for transferring the control codes and the authentication code to a physical layer hardware unit of the transceiver;

means for means for configuring assigned transmission parameters of the physical layer hardware unit based on the control codes; and

means for signaling a security violation in response to the control codes being inconsistent with the authentication code.